UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/804,852	03/19/2004	Lauri Paatero	915-008.022	7439

4955 7590 09/21/2009

WARE FRESSOLA VAN DER SLUYS & ADOLPHSON, LLP
BRADFORD GREEN, BUILDING 5
755 MAIN STREET, P O BOX 224
MONROE, CT 06468

EXAMINER	
NALVEN, ANDREW L	

ART UNIT	PAPER NUMBER
2434	

MAIL DATE	DELIVERY MODE
09/21/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/804,852	PAATERO, LAURI	
	Examiner	Art Unit	
	ANDREW L. NALVEN	2434	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 July 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1 and 4-12* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1, 4-12* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *09 July 2007* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1, 4-12 are pending.

Response to Arguments

2. Applicant's arguments filed 7/15/2009 have been fully considered but they are not persuasive.

3. Applicant has argued that Grohoski fails to teach the first logical interface is not accessible when data is transferred in the second logical interface. Examiner respectfully disagrees. Applicant has asserted that both the CPU and the cryptoprocessor can access the memory at the same time. However, Applicant has not pointed to any teaching within the reference that supports such an assertion. Applicant has cited portions of the reference referring to time T1, time T2, and some time between T1 and T2, but the CPU or cryptoprocessor does not access the first interface while the second interface is in use at any of these cited times. The Grohoski teaches the first logical interface is not accessible when data is transferred in the second logical interface (Grohoski, paragraph 0056, paragraphs 0061-0062). Grohoski teaches the limitation by teaching a CPU transferring data through a first and second interface. The limitation in question requires that the first logical interface (data transfer interface) not be accessible when the second logical interface (key transfer interface) is in use for transfer. Transfers are made through a set of shared memory (Grohoski, paragraph

0056). Accordingly, nothing can be read from the memory while a write operation is taking place. A computer memory cannot be read while it is being written to. As a result, Examiner maintains that Grohoski teaches the limitation in question.

4. Applicant further argues that Srinivasan fails to teach a "protected application." Examiner respectfully disagrees. Srinivasan teaches a configuration register arranged to indicate to the accelerator whether secure mode or normal mode is set by the processor and configured to receive mode setting instructions from a protected application, said processor arranged in the device (Srinivasan, paragraphs 0121-0123, 0127, 0133, paragraph 0139). Srinivasan teaches the application is protected by teaching application software setting parameters in registers (Srinivasan, paragraph 0121) which causes secure mode to be entered (Srinivasan, paragraphs 0121-0123, paragraphs 0133, 0139). The secure mode may then perform secure operations for the application including verifying additional components of the protected application (Srinivasan, paragraphs 0133, 0139).

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 1 and 5 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The cited claims are ambiguous because claim 5

requires that the two logical interfaces be carried by respective physical interfaces while parent claim 1 requires a single physical interface.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. **Claims 1, 4-12 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Grohoski et al US PGPub 2004/0225885 in view of Srinivasan et al US PGPub 2004/0158742.

7. **With regards to claims 1**, **11-12**, Grohoski teaches an electronic device comprising (Grohoski, paragraph 0056, paragraph 0106, crypto processor), an accelerator for accelerating cryptographic data processing operations, which acceleration is arranged with (Grohoski, paragraph 0056, higher speed encryption and decryption processes enabled using crypto coprocessor) a first logical interface over which data to be processed is provided (Grohoski, paragraphs 0061-0062, transfers crypto packet), a secure second logical interface over which cryptographic keys employed in the operation of processing data is provided (Grohoski, paragraph 0062, paragraph 0052, control queue, paragraphs 0056-0057, sharing access to registers and memory access units provides a secure connection, paragraph 0106, controlled access

to secure registers), and wherein the first logical interface and the secure second logical interface share a same physical interface (Grohoski, paragraph 0056, share same memory access units) and wherein the first logical interface is not accessible when data is transferred in the second logical interface (Grohoski, paragraph 0056, paragraphs 0061-0062). Grohoski fails to teach a configuration register arranged to indicate to the accelerator whether secure mode or normal mode is set by the processor arranged in the device. However, Srinivasan teaches a configuration register arranged to indicate to the accelerator whether secure mode or normal mode is set by the processor and configured to receive mode setting instructions from a protected application, said processor arranged in the device (Srinivasan, paragraphs 0121, 0127, 0133). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Srinivasan's method of providing secure operation modes for a processor because it offers the advantage of ensuring that only authorized application software is executed and only authorized multimedia content is rendered (Srinivasan, paragraph 0007).

8. **With regards to claim 4**, Grohoski as modified teaches the configuration register is further arranged such that is may be set in one of a plurality of possible encryption modes, the accelerator being arranged to operate in the encryption mode set in the register (Grohoski, paragraph 0116, encryption type field).

9. **With regards to claim 5**, Grohoski teaches the accelerator is arranged such that the first logical interface and the secure second logical interface are provided via respective physical interfaces (Grohoski, Figure 2 Items 215 and 210).

10. **With regards to claim 6**, Grohoski as modified teaches the first logical interface of the accelerator is arranged such that it is accessible by any application while the secure second logical interface of the accelerator is arranged such that it is accessible by protected applications only (Srinivasan, paragraphs 0007, 0121, 0127, 0133).

11. **With regards to claim 7**, Grohoski as modified teaches protected applications prevent other applications from accessing the accelerator (Grohoski, paragraph 0106).

12. **With regards to claim 8**, Grohoski as modified teaches protected applications are applications which are allowed to execute in the secure execution environment (Srinivasan, paragraphs 0121, 0127, 0133, Abstract).

13. **With regards to claim 9**, Grohoski as modified teaches storage circuitry arranged with at least one storage area in which protected data relating to device security is located (Grohoski, paragraph 0106), a processor arranged such that is may be set in one of at least two separate operating modes (Srinivasan, paragraphs 0007, 0121, 0127, 0133) and the device further arranged such that the processor is given access to said storage area when a normal processor operating mode is set (Srinivasan, paragraphs 0007, 0121, 0127, 0133) and the processor is denied access to said storage area when a normal processor operating mode is set (Srinivasan, paragraphs 0007, 0121, 0127, 0133) and the processor is capable of accessing the secure second logical interface of the accelerator when the secure processor operating mode is set (Srinivasan, paragraphs 0007, 0121, 0127, 0133).

14. **With regards to claim 10**, Grohoski as modified teaches the protected applications controlling the processor operation mode (Srinivasan, paragraph 0010).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ANDREW L. NALVEN whose telephone number is (571)272-3839. The examiner can normally be reached on Monday - Thursday 8-6, Alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on 571 272 3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Andrew L Nalven/
Primary Examiner, Art Unit 2434